UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/685,885	10/11/2000	Anders Johnson	108339-00010	5015

7590 06/15/2005

SQUIRE SANDERS & DEMPSEY LLP
14th FL
8000 Towers Crescent Drive
Tysons Corner, VA 22182-2700

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 06/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/685,885	JOHNSON, ANDERS	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/8/2005 has been entered. Claims 1, 15, and 25 were amended. Claims 1-33 are pending.

Docketing

Please note that the application has been redocketed to a different examiner. Please refer all future communications regarding this application to the examiner of record using the information supplied in the final section of the office action.

Response to Arguments

Applicant's arguments filed 4/26/2005 have been considered but most are moot in view of the new ground(s) of rejection.

The examiner will address the arguments to claims in which some limitations still apply, namely arguments directed towards claim 25. As per claim 25, applicant argues that Davis does not disclose determining a second bit string corresponding to the random number, wherein the second bit string is received from the manufacturer of the electronic component. This argument stems from the amendments to claim 25 and the examiner will make new rejections based on these amendments below. Applicant also argues that Davis does not disclose "encrypting the second bit string with a public key to

generate a third bit string." The examiner agrees. The key used for the encryption was a session key and not a public key, so the previous rejection for this limitation was improper. However, see new rejection for this limitation below.

The examiner notes that on page 21 of applicant's arguments filed 4/26/2005, applicant argues the limitations for claims 14, 24, and 33. On page 22, applicant argues the limitations for claims 14, 24, and 32. The examiner believes that applicant meant on page 22 to still argue the limitations for claim 33, and not claim 32 as claim 32 does not recite anything about a network switch or media access controller. Therefore, the examiner believes that the previous examiner's rejection for claim 32 is still valid and will address new rejections for claims 14, 24, and 33 below and not 32. The rejection for claim 32 from the last office action will be copied into this office action though.

The examiner notes applicant did not argue the rejections for claims 26-30. Therefore, the examiner assumes applicant agrees that the previous examiner's rejection of the limitations for these claims were proper and the examiner will incorporate the previous examiner's rejection for these claims into this office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 6-16, and 18-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tello (US 6,463,537) in view of Angelo et al (US 6,370,649).

Claim 1:

Tello discloses an apparatus for enabling functionality of a component (col 4, lines 57-63 and Fig 1), said apparatus comprising:

1. A random number generating module for generating a random number (col 8, lines 33-39 and col 15, lines 5-19). Note that usage of the RSA algorithm requires that there must be a random number generator.
2. A hash function module in communication with said random generating module (col 8, lines 10-16).
3. A host (i.e. computer, Fig 1) in communication with said random number generating module (col 8, lines 33-39 and col 15, lines 5-19).
4. At least one memory in communication with said host (col 9, lines 21-31).
5. An encryption module in communication with at least one memory (col 24, lines 46-50).
6. A comparing device in communication with said encryption module and said hash function module (col 16, lines 40-55).
7. Wherein said comparing device compares a first bit string to a second bit string to generate a function enable output for the component (col 15, lines 52-65 and col 16, lines 13-26).

Tello does not disclose wherein said host is configured to receive a guess passcode from a manufacturer of the component. However, Angelo teaches a computer system that implements a fail-safe password system that allows the manufacturer to securely supply a password to users (col 1, line 65-col 2, line 3). In light of this, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Tello's apparatus according to the limitations recited in claim 1. One of ordinary skill would have been motivated to incorporate Angelo's teachings because it allows for a hardened password security infrastructure (col 3, lines 18-20).

The examiner notes that even without Tello's teachings, it is common knowledge wherein a host is configured to receive a guess passcode from a manufacturer of a component—i.e. a cable decoder box, for example, receives entitlement messages from the cable company which reads on a guess passcode and enables a television set to display a descrambled show. It would also have been obvious to one of ordinary skill in the art to have modified Tello's apparatus according to the limitations recited in claim 1 in light of such common knowledge and one of ordinary skill would have been motivated to do so as it would provide a way for a manufacturer of a component who also sells subscription to digital content to maintain control of the digital content and only allow customers who have paid for the content to get access.

Claim 2:

Tello further discloses said hash function module further comprises a one-way hash function module configured to receive a pre-image input and output a hash value using a one-way has function algorithm (col 7, lines 64-66).

Claim 3:

Tello further discloses said encryption module further comprises a public key encryption module, said public key encryption module being configured to receive a public key and a guess passcode from said at least one memory area as inputs and generate a ciphertext bit string as an output (col 19, lines 12-25; col 24, lines 13-50; and col 37, lines 27-42).

Claim 4:

Tello further discloses wherein said at least one memory further comprises:

1. A guess register in communication with said host and said encryption module, said guess register being configured to receive a guess passcode from said host (col 24, lines 46-50).
2. A public key module in communication with said encryption module, said public key module being configured to store a public key therein (col 15, lines 6-9).

Claim 6:

Tello further discloses said apparatus further comprises a selecting device for selecting at least one of the function enable output and bonding option output (col 9, lines 33-44).

Claim 7:

Tello further discloses said selecting device further comprises an OR gate having at least one input for receiving the function enable output and the bonding option output (col 13, lines 1-56; col 19, lines 12-25; and col 37, lines 27-42).

Claim 8:

Tello further discloses said bonding option circuit comprising a pull up resistor in communication with the OR gate and a power supply and a switch in communication with a ground potential and said OR gate (col 9, lines 59-62 and col 12, line 65-col 13, line 5).

Claim 9:

Tello further discloses said selecting device further comprises:

1. A multiplexer having at least one multiplexer input in communication with the comparing device and a multiplexer output (col 13, lines 5-49).
2. A selection circuit in communication with the at least one multiplexer input (col 13, lines 5-49).
3. A bonding option circuit in communication with the at least one multiplexer input (col 9, lines 33-49 and col 12, lines 35-45).
4. Wherein said multiplexer is configured to receive a selection input from the selection circuit that is used to determine whether to enable functionality of said component in accordance with the bonding option output or the function enable output (col 9, lines 33-49; col 12, lines 35-45; col 19, lines 12-25; and col 37, lines 27-42).

Claim 10:

Tello further discloses said selection circuit further comprises:

1. At least one first non-volatile memory location having at least one first selection bit stored therein (col 7, line 63-col 8, line 4 and col 15, lines 1-36).
2. At least one second non-volatile memory location having at least one second selection bit stored therein (col 8, lines 40-49 and col 15, lines 1-36).
3. An OR gate having a first input, a second inverted input, and a logic output, said first input being in communication with said at least one first non-volatile memory location and said second inverted input being in communication with said at least one second non-volatile memory location (col 19, lines 12-25 and col 37, lines 27-42).
4. Wherein said selection circuit is configured to generate a selection indicator on the logic output of the OR gate in accordance with the at least one first selection bit and said at least one second selection bit (col 13, lines 6-58).

Claim 11:

Tello further discloses said first bit string further comprises a ciphertext bit string generated by the encryption module (col 15, lines 52-65; col 16, lines 13-26; and col 20, lines 1-23).

Claim 12:

Tello further discloses said second bit string further comprises a hash value generated by said hash function module (col 16, lines 30-32).

Claim 13:

Tello does not explicitly disclose said comparing device further comprises a comparator. However, a comparator must be used or a comparison would not be possible.

Claim 14:

Tello further discloses said component further comprises at least one of a network switch and a media access controller (col 11, lines 49-52).

Claim 15:

Tello discloses a component for selectively enabling functionality of an electronic device, said component comprising:

1. Means for generating a random bit string (col 8, lines 33-39 and col 15, lines 5-19).
2. A hash function module in communication with said means for generating (col 8, lines 10-16).
3. Means for acquiring a guess passcode in communication with said means for generating (col 9, lines 20-24 and col 24, lines 46-50).
4. An encryption module in communication with said means for acquiring (col 24, lines 46-50).
5. A comparing device in communication with said encryption module and said hash function module, said comparing device having an output for transmitting a functionality enable signal therefrom (col 15, lines 52-65; col 16, lines 40-55; and col 16, lines 13-26).

Tello does not disclose wherein the means for acquiring the guess passcode is configured to acquire the guess passcode from a manufacturer of the electronic device. However, for the same reasons and motivations given in claim 1, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Tello's component according to the limitations recited in claim 15 in light of Angelo's teachings (or in light of common knowledge in the art).

Claim 16:

Tello does not explicitly disclose wherein said means for generating further comprises a random number generating module, wherein said module is configured to receive an initiate signal and output a random number. However, Tello discloses usage of the RSA encryption algorithm (col 8, lines 33-39 and col 15, lines 5-19), which requires the usage of a random number generating module. The module must be able to output a random number when an initiate signal is received.

Claim 18:

The limitation of claim 18 is substantially similar to claim 2 and is rejected for the same reasons.

Claim 19:

Tello further discloses wherein said means for acquiring a guess passcode further comprises:

1. A host in communication with said means for generating (col 15, lines 7-11).
2. A guess register in communication with said host (col 9, 20-24 and col 24, lines 46-50).

3. The random bit string (col 9, lines 20-25 and col 15, lines 20-27).

Tello does not disclose wherein said host is configured to receive a guess passcode from a manufacturer corresponding to the random bit string. However, for the same reasons and motivations given in claim 1, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Tello's component according to the limitations recited in claim 19 in light of Angelo's teachings (or in light of common knowledge in the art).

Claim 20:

Tello further discloses wherein said encryption module further comprises:

1. A public key encryption module (col 15, lines 6-9).
2. A public key module in communication with said public key encryption module (col 15, lines 6-19).
3. Wherein said public key encryption module is configured to receive a public key from said public key module and a guess passcode from said means for acquiring, and generate a ciphertext bit string therefrom (col 8, lines 5-9; col 19, lines 12-25; and col 37, line 26-col 38, line 7).

Claim 21:

Tello further discloses said component further comprising:

1. A bonding option circuit in communication with said comparing device (col 9, lines 33-49 and col 12, lines 35-45).

2. An OR gate in communication with said comparing device (col 12, line 67-col 13, line 5).
3. Wherein said OR gate is configured to select the functionality enable signal from the comparator or an output from the bonding circuit in order to generate a final enable output (col 9, lines 33-49 and col 13, lines 1-56).

The examiner also notes that the limitation as recited in claim 21 is an obvious way of using an OR gate to generate a final enable output as the output from the comparing device naturally would enable a device on a successful comparison while the output from the bonding option circuit can be used as a bypass circuit, which are known in the art and one of ordinary skill would be motivated to use one for testing purposes.

Claim 22:

Claim 22 recites limitations substantially similar to claim 8 and is rejected for the same reasons.

Claim 23:

Claim 23 recites limitations substantially similar to claim 13 and is rejected for the same reasons.

Claim 24:

Claim 24 recites limitations substantially similar to claim 14 and is rejected for the same reasons.

Claims 5 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tello (US 6,463,537) in view of Angelo et al (US 6,370,649) and further in view of Couch et al (US 5,383,143).

Claims 5 and 17:

Tello and Angelo do not explicitly disclose the limitations as recited in claims 5 and 17. However, the examiner asserts that it is well known in the art of digital logic to use a linear feedback shift register to generate random numbers. This is also disclosed by Couch (col 5, lines 7-9). Further, the use of NAND gates and inverters in communication with each other as well as other digital circuitry are also well known. The use of a NAND gate (as well as other types of logic gates) in the art of digital logic to receive an activation pulse to control other digital circuitry is also well known and is common practice in the art. In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Tello and Angelo's combination invention according to the limitations recited in claim 5 and 17. One of ordinary skill would have been motivated to do so as because of common practice in the art and because Couch discloses the use of a linear feedback shift register to implement a random number generator would result in an efficient design that has a large degree of functionality in a small circuit surface area (col 4, lines 33-40).

Claims 25-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al (US 5,577,121) in view of Tello (US 6,463,537) and further in view of Angelo et al (US 6,370,649)

Claim 25:

Davis discloses a method for enabling functionality of an electronic component, said method comprising the steps of:

1. Generating a random number (col 13, lines 6-8).
2. Calculating a first bit string from the random number (col 13, lines 9-10 and 18-25).
3. Determining a second bit string corresponding to the random number (col 13, lines 36-46).
4. Encrypting the second bit string with a key to generate a third bit string (col 13, line 36-42).
5. Comparing the third bit string to the first bit string to determine at match (col 13, line 53-55).
6. Outputting a function enable signal in accordance with the comparison (col 13, lines 53-55). The confirmation signal represents the enable signal.

Note that the above limitations were rejected in the last office action and as applicant did not argue them, the examiner assumes applicant agrees the rejection of these limitations were proper. Davis does not disclose the second bit string was encrypted using a public encryption key.

However, the examiner asserts that the use of public encryption keys for encryption purposes was well known in the art at the time the applicant's invention was made. It would have been obvious to one of ordinary skill to have used a public encryption key as the type of encryption key used is an arbitrary choice. Further, Tello discloses encryption using a public encryption key (col 8, lines 33-39). In light of this, it would have been obvious to one of ordinary skill to have modified Davis's method to encrypt the second bit string with a public key to generate a third bit string. One of ordinary skill would have been motivated to incorporate Tello's teachings because Tello discloses a similar enabling invention as Davis and Tello discloses that almost any key algorithm can be used without materially changing the functionality of the invention (col 8, lines 36-39), therefore the use of a public key is an arbitrary choice.

Davis also does not disclose wherein the step of determining the second bit string comprises receiving the second bit string from a manufacturer of the electronic component. However, for the same reasons and motivations given in claim 1, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified the combination method of Davis and Tello according to the limitations recited in claim 25 in light of Angelo's teachings (or in light of common knowledge in the art).

Claim 26:

With respect to claim 26, Davis meets the limitation of "wherein said step of calculating a first bit string further comprises calculating a hash value of said random number" is met on column 17, lines 42-52 and column 14, lines 43-47). The examiner

notes that applicant did not argue this limitation in the last office action, so assumes applicant agrees Davis meets this limitation.

Claim 27:

With respect to claim 27, Davis meets the limitation of "transmitting the random number to a manufacturer" on col 13, lines 8-10; "calculating a guess passcode corresponding to the random number" is met on col 13, lines 18-22; and "receiving the guess passcode in a host" is met on col 13, lines 23-29. The examiner notes that applicant did not argue this limitation in the last office action, so assumes applicant agrees Davis meets this limitation.

Claim 28:

With respect to claim 28, Davis meets the limitation of "receiving a guess passcode from a host" on column 13, lines 55-60 and "receiving a public key and encrypting the guess passcode and the public key to generate a ciphertext bit string" is met on col 13, lines 55-63. The examiner notes that applicant did not argue this limitation in the last office action, so assumes applicant agrees Davis meets this limitation.

Claim 29:

With respect to claim 29, Davis meets the limitation of "receiving the third bit string at a first input of a comparator; and receiving the first bit string at a second input of the comparator; determining if the first bit string matched the second bit string" on col 13, lines 66-67 and col 14, lines 1-3. Davis also meets the limitation of "outputting a match signal if a match is determined (col 14, lines 3-7). The examiner notes that

applicant did not argue this limitation in the last office action, so assumes applicant agrees Davis meets this limitation.

Claim 30:

With respect to claim 30, the limitation of "wherein said outputting step further comprises the step of determining a final output enable signal from a bonding option output signal and the function enable signal" is met inherently on column 14, lines 3-10. The examiner notes that applicant did not argue this limitation in the last office action, so assumes applicant agrees Davis meets this limitation.

Claim 31:

Davis does not explicitly disclose the limitations recited in claim 31. However, claim 31 contains limitations substantially similar to the limitations recited in claim 21 which were rejected using Tello. Therefore, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have incorporated Tello's teachings with Davis's method according to the limitation recited in claim 31. One of ordinary skill would have been motivated to incorporate Tello's teachings as Tello discloses that his invention would provide for a means for controlling access to a computer and sensitive data stored on it at the pre-boot phase and during operation of the computer (col 4, lines 57-61).

Claim 32:

With respect to claim 32, Davis meets the limitation of "wherein said transmitting step further comprises communicating with the manufacturer through at least one of an internet connection, a dial up connection, and a voice connection to obtain the guess

passcode" on col 17, lines 18-22. The examiner notes that applicant did not argue this limitation in the last office action, so assumes applicant agrees Davis meets this limitation.

Claim 33:

Davis does not explicitly disclose the limitation recited in claim 33. However, claim 33 contains limitations substantially similar to the limitations recited in claim 14 which were rejected using Tello. Therefore, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have incorporated Tello's teachings with Davis's method according to the limitation recited in claim 31. One of ordinary skill would have been motivated to incorporate Tello's teachings as Tello discloses that his invention would provide for a means for controlling access to a computer and sensitive data stored on it at the pre-boot phase and during operation of the computer (col 4, lines 57-61).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100